AMENDMENTS TO THE CLAIMS

Amended claims follow:

1. (Currently Amended) A network adapter system, comprising:

a processor positioned on a network adapter coupled between an end-point computer and a network, the network adapter capable of being installed on the end-point computer;

wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses;

wherein the system is operable such that the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

wherein the system is operable such that the virus signature files are stored on non-volatile solid state memory on the network adapter;

wherein the processor is user-configured;

wherein the processor determines whether received packets are of interest, passes the received packets that are not of interest to the end-point computer, and scans the received packets that are of interest;

wherein the system is operable such that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter;

wherein the system is operable such that if the received packets that are of interest fail the scanning, an alert is displayed which provides remedy options;

wherein the system is operable such that the received packets are of interest based on an associated protocol;

wherein the system is operable such that the received packets that are not of interest bypass the scanning;

wherein the system is operable such that scanning the received packets that are of interest is prioritized based on a file type associated with the received packets.

2. (Cancelled)

3. (Previously Presented) The network adapter system as recited in claim 1, wherein the processor is user-configured locally.

4. (Previously Presented) The network adapter system as recited in claim 1, wherein the processor is user-configured remotely via a network connection with the network adapter.

5. (Previously Presented) The network adapter system as recited in claim 1, wherein the processor is user-configured only after verification of a password.

6. (Previously Presented) The network adapter system as recited in claim 1, wherein a manner in which the scanning is performed is user-configured.

7. (Previously Presented) The network adapter system as recited in claim 1, wherein settings of the network adapter are user-configured.

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12. (Previously Presented) The network adapter system as recited in claim 1, wherein the processor denies received packets that fail the scan.

13. (Original) The network adapter system as recited in claim 1, wherein the scan is performed based on user settings.

14. (Currently Amended) A method for scanning network traffic on a network adapter, comprising:

receiving packets at a network adapter including a processor positioned thereon, the network adapter installed on an end-point computer;

virus scanning and content scanning of the packets utilizing the processor, the content scanning including scanning for unwanted content other than viruses; and

conditionally taking security measures if the packets fail the scan;

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter;

wherein the processor is user-configured;

wherein the processor determines whether the received packets are of interest, passes the received packets that are not of interest to the end-point computer, and scans the received packets that are of interest;

wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter;

wherein if the received packets that are of interest fail the scanning, an alert is displayed which provides remedy options;

wherein the received packets are of interest based on an associated protocol;

wherein the received packets that are not of interest bypass the scanning;

wherein scanning the received packets that are of interest is prioritized based on a file type associated with the received packets.

15. (Cancelled)

16. (Previously Presented) The method as recited in claim 14, wherein the processor is user-configured locally.

17. (Previously Presented) The method as recited in claim 14, wherein the processor is user-configured remotely via a network connection with the network adapter.

18. (Previously Presented) The method as recited in claim 14, wherein the processor is user-configured only after verification of a password.

19. (Previously Presented) The method as recited in claim 14, wherein a manner in which the scanning is performed is user-configured.

20. (Previously Presented) The method as recited in claim 14, wherein the settings of the network adapter are user-configured.

21. (Cancelled)

22. (Cancelled)

23. (Cancelled)

24. (Cancelled)

25. (Previously Presented) The method as recited in claim 14, wherein the processor denies received packets that fail the scan.

26. (Original) The method as recited in claim 14, wherein the scan is performed based on user settings.

27. (Currently Amended) A system ~~for scanning network traffic on a network adapter~~, comprising:

network adapter means for receiving packets, the network adapter means installed on an end-point computer;

processor means positioned on the network adapter means for virus scanning and

content scanning of the packets, the content scanning including scanning for unwanted content other than viruses; and

means for conditionally taking security measures if the packets fail the scan;

wherein the system is operable such that the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

wherein the system is operable such that the virus signature files are stored on non-volatile solid state memory on the network adapter means;

wherein the processor means is user-configured;

wherein the processor means determines whether the received packets are of interest, passes the received packets that are not of interest to the end-point computer, and scans the received packets that are of interest;

wherein the system is operable such that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter means;

wherein the system is operable such that if the received packets that are of interest fail the scanning, an alert is displayed which provides remedy options;

wherein the system is operable such that the received packets are of interest based on an associated protocol;

wherein the system is operable such that the received packets that are not of interest bypass the scanning;

wherein the system is operable such that scanning the received packets that are of interest is prioritized based on a file type associated with the received packets.

28. (Currently Amended) A system ~~for scanning network traffic on a network adapter~~, comprising:

network adapter means for receiving packets, the network adapter means being installed on an end-point computer;

logic positioned on the network adapter means for virus scanning and content scanning of the packets, the content scanning including scanning for unwanted content other than viruses; and

logic for conditionally taking security measures if the packets fail the scan;

wherein the system is operable such that the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

wherein the system is operable such that the virus signature files are stored on non-volatile solid state memory on the network adapter means;

wherein the logic is user-configured;

wherein the logic determines whether the received packets are of interest, passes the received packets that are not of interest to the end-point computer, and scans the received packets that are of interest;

wherein the system is operable such that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter means;

wherein the system is operable such that scanning the received packets that are of interest is prioritized based on a file type associated with the received packets;

wherein the system is operable such that the received packets are of interest based on an associated protocol;

wherein the system is operable such that the received packets that are not of interest bypass the scanning.

29. (Currently Amended) A network adapter system, comprising:

a processor positioned on a network adapter coupled between an end-point computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module, the network adapter being installed on the end-point computer; and

a user interface driver for identifying network traffic of interest transmitted between the end-point computer and the network;

wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses;

wherein the system is operable such that the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

wherein the system is operable such that the virus signature files are stored on non-volatile solid state memory on the network adapter;

wherein the network adapter receives the network traffic;

wherein the processor is user-configured;

wherein the processor determines whether the received network traffic is of interest, passes the received network traffic that is not of interest to the end-point computer, and scans the received network traffic that is of interest;

wherein the system is operable such that a predetermined amount of the received network traffic is assembled for determining whether the received network traffic is of interest, the received network traffic including network traffic received at the network adapter;

wherein the system is operable such that scanning the received network traffic of interest is prioritized based on a file type associated with the received network traffic;

wherein the system is operable such that the received ~~packets are~~network traffic is of interest based on an associated protocol;

wherein the system is operable such that the received network traffic that is not of interest bypasses the scanning.

30. (Previously Presented) The network adapter system as recited in claim 1, wherein the content scanning enforces operational policies of an organization.

31. (Currently Amended) The network adapter system as recited in claim 30, wherein the operational policies include detecting entities ~~selected from a group consisting~~including at least one of harassing content, pornographic content, junk e-mails, and misinformation.

32. (Cancelled)

33. (Previously Presented) The network adapter system as recited in claim 1, wherein the non-volatile solid state memory is user-protected by configuring a network adapter BIOS with a password that only a user can change.

34. (Previously Presented) The network adapter system as recited in claim 1, wherein the received packets that are of interest include executable files.

35. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes a Peripheral Component Interconnect (PCI) card.

36. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes an Industry Standard Architecture (ISA) card.

37. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes an Integrated Services Digital Network (ISDN) adapter.

38. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes a cable modem adapter.

39. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes a broadband adapter.

40. (Currently Amended) The network adapter system as recited in claim 1, wherein the unwanted content ~~is selected from a group consisting~~includes at least one of harassing content, pornographic content, junk e-mails, and misinformation.

41. (Previously Presented) The network adapter system as recited in claim 1, wherein the unwanted content includes harassing content, pornographic content, junk e-mails, and misinformation.

42. (Cancelled)

43. (Cancelled)

44. (Previously Presented) The network adapter system as recited in claim 29, wherein the packet assembly module utilizes header information associated with received network traffic for assembling data fields of the received network traffic.

45. (Cancelled)

46. (Cancelled)

47. (New) The network adapter system as recited in claim 1, wherein the received packets are of interest based on the associated protocol, a source of the received packets, a timing of the received packets, and contents of the received packets.

48. (New) The network adapter system as recited in claim 1, wherein the bypassing of the scanning includes bypassing a scanner and random access memory (RAM) of the processor, and communicating directly with a network driver of the end-point computer.

49. (New) The network adapter system as recited in claim 1, wherein the displaying of the alert includes sending the alert to a user interface driver or the end-point computer.

50. (New) The network adapter system as recited in claim 1, wherein the prioritizing of the scanning of the received packets that are of interest based on the file type associated with the received packets includes prioritizing an executable file type before an image file type.